Quantum Computation with Coherent Spin States and the Close Hadamard Problem

Mark R. A. Adcock,[1] Peter Høyer,[1,2] and Barry C. Sanders[1]
[1] *Institute for Quantum Information Science, University of Calgary, Calgary, Alberta, Canada, T2N 1N4. Email:* mkadcock@qis.ucalgary.ca
[2] *Department of Computer Science, University of Calgary, 2500 University Drive N.W., Calgary, Alberta, Canada, T2N 1N4. Email:* hoyer@ucalgary.ca.

We study quantum algorithms inspired by the continuously-parameterized yet finite-dimensional Hilbert space of a coherent spin system. We show that the highest-squeezed spin state possible can be approximated by a superposition of two states thus transcending the usual model of using a single basis state as algorithm input. As a particular example, we show that the close Hadamard oracle-decision problem, which is related to the Hadamard codewords of digital communications theory, can be solved quantitatively more efficiently using this computational model than by any known classical algorithm.

PACS numbers: 03.67.Ac

I. INTRODUCTION

Ever since the remarkable discovery that quantum mechanical systems can in principle be used for computational purposes by pioneers such as Benioff [1], Feynman [2], and Deutsch [3], researchers have considered the feasibilities of implementing such computations in a rich variety of physical models. These models include phenomena such as light, electrons, atomic nuclei each of which have degrees of freedom such as position, path or spin into which quantum information can be encoded, processed and measured. The measurement spectrum can be discrete, for example measuring spin up or down or position being left or right, or continuous, for example measuring the angle of the spin axis or where on a line the particle is located.

This distinction between whether the spectrum of measurement, or preparation, is discrete or continuous is at the heart of the difference between discrete variable and continuous variable versions of quantum information. A system is considered to be continuous variable when either the spectrum of preparation or the spectrum of measurement is continuous.

The processing of quantum information in discrete variable systems has the advantage of being amenable to the theory of quantum error correction. Discrete variable systems, where experimentalists have successfully demonstrated the potential computational power of quantum systems, include trapped ions [4], liquid nuclear magnetic resonance [5] and quantum dots [6].

Processing with continuous variable systems has the advantage of being amenable to many physical preparation and measurement procedures that feature continuous tunability. Continuous variable quantum information is the less studied of the two types yet offers new insights that can engender creative thinking about new quantum algorithms. Given the significant progress that has been made in recent years in understanding and controlling quantum optics systems [7–15], there seems to be a potential for further progress in realizing quantum computation using continuous variables.

Continuous variable studies are typically linked to harmonic oscillators because quantum optics has powerful tools to work prepare, process and measure optical field modes [16], which are analogous to harmonic oscillators. Quantum optics also offers an easy-to-implement Fourier transform, which maps canonical position states to canonical momentum states. The duality between position and momentum states is evident in that the magnitude of the overlap between any position and any momentum state is constant regardless of the choice of position and momentum states.

This duality is only exact for continuous position and momentum over an unbounded spectrum, which is an unattainable ideal. A well-know example of this duality is the time-bandwidth uncertainty relation of Fourier transforms. This inherent uncertainty relation limits the performance of quantum algorithms implemented over qudits encoded into position states of a single harmonic oscillator [17, 18]. Encoding over sufficiently many harmonic oscillators [19] ameliorates this limitation somewhat.

Continuous variable quantum information processing may be thought of as a model of quantum computation. The circuit model was the first such model [20], and the circuit and one-way quantum models are examples of different models [21], which are distinguished by different processing methods. The continuous variable model of quantum computation has inspired a continuous variable Deutsch-Jozsa algorithm [7, 17, 18]. Here we explore another continuous variable model of quantum computation based on coherent spin states and show that it can inspire a new algorithm.

Although fixed total spin states span a finite-dimensional Hilbert space, continuous encoding is possible using the continuously-parameterized, squeezed spin coherent states [22], which are analogous to the squeezed coherent states of the harmonic oscillator [23–25]. The finite-dimensional Hilbert space has the effect that squeezing of coherent spin states is Heisenberg-limited [22], unlike the coherent states of the harmonic oscillator where the allowed amount of squeezing is un-

bounded. We consider encoding quantum information into the highest-squeezed spin state that can be achieved.

We demonstrate that this optimally squeezed state may be approximated well by a superposition of two discrete states, thus idealizing the computation model beyond encoding into squeezed spin states while keeping the spin gates. This approach allows us to discover a new algorithm that can be processed using the circuit model of quantum computation. Our investigation of a continuous variable spin model of quantum computation has thus inspired us to find a new quantum algorithm.

Our paper is presented as follows. In Sec. II, we introduce an oracle decision problem parameterized by $N = 2^n$-bit strings. We refer to this new oracle decision problem as the *close Hadamard problem*, which is related to the digital coding techniques employed in classical communications [26, 27]. The close Hadamard problem is inspired by the continuous variable operators and displacement and squeezing tools used in the continuously-parameterized, infinite-dimensional Hilbert space case adapted to the continuously-parameterized, finite-dimensional Hilbert space case.

In Sec. III, we introduce the spin-system model. We discuss the preparation of coherent spin states and how to use Q-functions for spin systems, parameterized by the spherical angles, as a visualization aid. We introduce the concept of spin squeezing and show how squeezing changes the amplitude distribution of the individual spin states. We show, that for a particular coherent spin state, the limiting squeezed state is asymptotically approximated by a symmetric superposition of two discrete states with constant error independent of the size of the Hilbert space. We use this superposition as the algorithm input state.

In Sec. IV, we demonstrate that our quantum algorithm efficiently solves the *restricted* close Hadamard problem with certainty in a single oracle query and also solves the *unrestricted* close Hadamard problem with arbitrarily small error in a constant number of queries. We also show that any known classical algorithm requires $\Omega(n)$ queries. In the restricted case in particular, this speed-up is the result of the cancellation of bit errors of certain patterns and results from using a superposition of two states as algorithm input.

In Sec. V, we discuss generalization of the computational model by showing that if the Hadamard operation is replaced by the discrete Fourier transformation, the oracle decision problem changes and is related to what can be thought of as fractional bits. We conclude in Sec. VI that this model of quantum computation can be used to inspire the efficient solution of additional problems.

II. ORACLE DECISION PROBLEMS AND THE CLOSE HADAMARD PROBLEM

Quantum algorithms for the efficient solution of oracle decision problems are of historical importance in quantum information [3, 28]. The Deutsch-Jozsa problem in particular has been studied in both discrete and continuous variable settings [7, 17, 18, 28]. We are inspired by the continuous variable quantum algorithm used to solve the Deutsch-Jozsa problem, where logical states are a continuously-parameterized in a *infinite*-dimensional Hilbert space. Here we explore this continuous variable quantum algorithm where the logical states are continuously-parameterized in the *finite*-dimensional Hilbert space of a spin system.

This continuously-parameterized spin model of quantum computation naturally yields to a symmetric superposition of two basis states as the logical state. Returning to a discrete representation inspires us to discover a new oracle decision problem, which we refer to as the close Hadamard problem.

A. Oracle Decision Problems

Oracle decision problems are related to oracle identification problems, which are usually presented in terms of the problem of identifying a unique function f. The function f maps $N = 2^n$-bit strings to a single bit

$$f : \{0,1\}^n \mapsto \{0,1\}. \tag{1}$$

Any Boolean function on n bits can also be represented by a string of $N = 2^n$ bits, in which the i^{th} bit z_i is the value of the function on the i^{th} bit string, taken in lexicographical order. The challenge of the oracle identification problem is to identify a unique N-bit string from a set of size 2^N by making the fewest queries to an oracle.

Oracle decision problems are simpler than oracle identification problems because the function or string does not have to be identified explicitly. Rather the problem is to identify which of two mutually disjoint sets contains the string. For our analysis, the oracle decision problem is defined as follows.

Definition 1. *An oracle decision problem is specified by two non-empty, disjoint subsets $A, B \subset \{0,1\}^N$. Given a string $z \in A \cup B = C$, the oracle-decision problem is to determine whether $z \in A$ or $z \in B$ with the fewest queries to the oracle possible.*

B. The Close Hadamard Problem

In this subsection, we specify the particular sets A, B and C required by Definition 1 for the close Hadamard problem. We refer to this decision problem as *close* because we are interested in strings that are *close* in the

sense of Hamming distance to the $N = 2^n$-bit strings referred to as Hadamard codewords [26, 29].

The problem of discriminating between codewords received after transmission over a noisy channel is well-known in classical digital coding theory employing linear block codes [30]. Linear block codes are characterized by the triplet $[N, k, t]$, where N is the total length of the codeword; $k < N$ is the amount of information coded, and $t - 1$ is the number of errors that the code can correct.

The Hadamard code is a linear block code with $N = 2^n$, $k = n + 1$, and $t = N/4 - 1$. The Hadamard code has a poor information rate k/N, but it has excellent error-correcting capability. Because of this latter feature, the $[32, 6, 7]$ Hadamard code was used to encode picture information on Mariner space craft missions [29].

For $N = 2^n$, the matrix comprising Hadamard codewords is

$$\mathsf{W}^{(N)} = \log_{(-1)}\left[\sqrt{N}\mathsf{H}^{\otimes n}\right], \tag{2}$$

where $\mathsf{H}^{\otimes n}$ is the familiar Hadamard matrix of quantum computation [31]. The expression $\log_{(-1)}[x]$ is the logarithm of x to the base -1, and, if $x = (-1)^y$, then $y = \log_{(-1)}[x]$.

For counting purposes we define the set $\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$. For $j \in \mathbb{Z}_N$, the j^{th} Hadamard codeword corresponds to the j^{th} row of the matrix $\mathsf{W}^{(N)}$ and is expressed as $W_j^{(N)}$. For example

$$\mathsf{W}^{(4)} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \tag{3}$$

and $W_3^{(4)} = 0110$. Note that all Hadamard codewords are balanced with the exception of $W_0^{(N)}$, which is constant. Also note that all N Hadamard codewords are separated from each other by Hamming distance

$$d\left(W_j^{(N)}, W_k^{(N)}\right) = N/2. \tag{4}$$

An arbitrary string $z \in \{0,1\}^N$ having Hamming distance $d\left(z, W_j^{(N)}\right) < N/4$ from any Hadamard codeword is said to be within the $t-$error-correcting capability of the Hadamard code [27].

In our analysis, we introduce Hadamard codewords with two types of bit errors: *unrestricted* errors and *restricted* errors. Unrestricted bit errors can occur at any of the N bit positions, whereas restricted errors are limited to $N/2$ specific bit positions.

1. Codewords with unrestricted errors

The codewords having *unrestricted* errors are the strings having Hamming distance d from any Hadamard codeword $W_j^{(N)}$. We define the set of codewords with errors specified with respect to any particular codeword through the use of an error syndrome, which represents all the possible ways an error of d bits can occur.

The error syndrome for d unrestricted errors is

$$U_d = \left\{z \in \{0,1\}^N \mid |z| = d\right\}. \tag{5}$$

The set of codewords having d unrestricted errors with respect to the j^{th} codeword is

$$\Xi_{j,d}^{(N)} = \left\{z \oplus W_j^{(N)} \mid z \in U_d\right\}, \tag{6}$$

and the set of all correctable codewords with zero to $N/16$ unrestricted errors is

$$\Xi_j^{(N)} = \left\{\Xi_{j,m}^{(N)} \mid m \in \mathbb{Z}_{N/16}\right\}. \tag{7}$$

We proceed in a similar manner with the definition of the Hadamard codewords having restricted errors, which are a subset of $\Xi_j^{(N)}$.

2. Codewords with restricted errors

The codewords having *restricted* errors are the strings with Hamming distance d from Hadamard codeword $W_j^{(N)}$, but the errors are restricted to the $N/2$ specific bit positions where the codeword $W_{N-1}^{(N)}$ contains a one. The error syndrome for d *restricted* errors is

$$R_d = \left\{z \in \{0,1\}^N \mid |z| = d \text{ and } z \preccurlyeq W_{N-1}^{(N)}\right\}. \tag{8}$$

We say that a vector $a \in \{0,1\}^N$ is dominated by a vector $b \in \{0,1\}^N$, denoted $a \preccurlyeq b$, if whenever $a_i = 1$ then also $b_i = 1$. The set of codewords having d restricted errors with respect to the j^{th} codeword is

$$\tilde{\Xi}_{j,d}^{(N)} = \left\{z \oplus W_j^{(N)} \mid z \in R_d\right\}. \tag{9}$$

We present two examples of the sets given by Eq. (9).

For the $N = 8$ case where there is a single restricted error, we have $W_7^{(8)} = 01101001$, and, for the particular codeword $W_4^{(8)} = 00001111$,

$$\tilde{\Xi}_{4,1}^{(8)} = \{01001111, 00101111, 00000111, 00001110\}. \tag{10}$$

Inspection of the set given in Eq. (10) reveals the error alignment with the bit positions where $W_7^{(8)} = 1$.

For $N = 8$ where there are two restricted errors, the errors may occur at any two of four possible possible bit positions represented as $\{a, b, c, d\}$, for which there are the $\binom{4}{2} = 6$ distinct bit error pairings $\{ab, ac, ad, bc, bd, cd\}$. The codewords with two errors in this case are

$$\begin{aligned}\tilde{\Xi}_{4,2}^{(8)} = \{&00000110, 00100111, 00101110, 01000111, \\ &01001110, 01101111\}.\end{aligned} \tag{11}$$

For the general case, the set having m-tuple restricted errors has size $\left|\tilde{\Xi}_{j,m}^{(N)}\right| = \binom{N/2}{m}$.

The set of all correctable codewords with zero to $N/4$ restricted errors with respect to the j^{th} Hadamard codeword is

$$\tilde{\Xi}_j^{(N)} = \left\{ \tilde{\Xi}_{j,m}^{(N)} \mid m \in \mathbb{Z}_{N/4} \right\}. \tag{12}$$

The size of this set is exponential in N since

$$\begin{aligned} \left|\tilde{\Xi}_j^{(N)}\right| &= \sum_{m=0}^{N/4-1} \binom{\frac{N}{2}}{m} \\ &= \frac{1}{2}\left[2^{\frac{N}{2}} - \binom{\frac{N}{2}}{\frac{N}{4}} \right]. \end{aligned} \tag{13}$$

We now define two variations of the close Hadamard problem in terms of Definition 1.

Problem 1. *Given the set of codewords $\tilde{A} = \tilde{\Xi}_{N/2-1}^{(N)}$, which contains strings that are close (in the restricted sense) to the Hadamard codeword $W_{N/2-1}^{(N)}$ and the set of codewords $\tilde{B} = \tilde{\Xi}_k^{(N)}$, which contains strings that are close (in the restricted sense) to any other Hadamard codeword $W_k^{(N)}$ with $k \in \mathbb{Z}_{N/2-1}$ and a string z randomly selected with uniform distribution μ such that $z \in_\mu \tilde{C} = \tilde{A} \cup \tilde{B}$, the* ***restricted close Hadamard problem*** *is to determine if $z \in \tilde{A}$ or $z \in \tilde{B}$ with the fewest oracle queries.*

In our formulation of Problem 1, we have made a technical assumption by setting $j = N/2-1$ in our definition of set $\tilde{A}$. We could have selected any other $j \in \mathbb{Z}_{N/2}$ as long as we excluded the selection from the definition of set $\tilde{B}$. We make this assumption because our quantum algorithm requires the measurement of some qubit. We have arbitrarily, and without loss of generality, set it to the qubit that corresponds to $j = N/2-1$. The same assumption is made in our formulation of Problem 2.

Problem 2. *Given the set of codewords $A = \Xi_{N/2-1}^{(N)}$, which contains strings that are close (in the unrestricted sense) to the Hadamard codeword $W_{N/2-1}^{(N)}$ and the set of codewords $B = \Xi_k^{(N)}$, which contains strings that are close (in the unrestricted sense) to any other Hadamard codeword $W_k^{(N)}$ with $k \in \mathbb{Z}_{N/2-1}$ and a string z randomly selected with uniform distribution μ such that $z \in_\mu C = A \cup B$. The* ***unrestricted close Hadamard problem*** *is to determine if $z \in A$ or $z \in B$ with the fewest oracle queries.*

C. Quantum Algorithm for Oracle Decision Problems

The quantum circuit represented in Fig. 1 solves the Deutsch-Jozsa oracle decision problem employing logical states encoded in the infinite-dimensional Hilbert space of the harmonic oscillator [17, 18]. In this case, $\Psi(x)$ is a square-integrable function of the continuous position x.

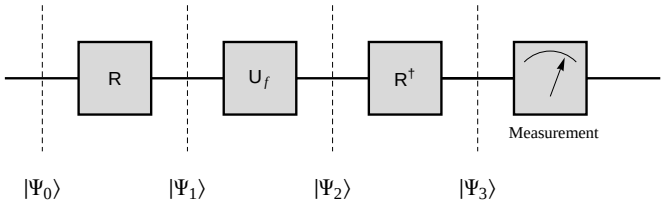

FIG. 1: Single-mode quantum circuit for oracle decision problems [17].

A key aspect of the approach is the physical accessibility of the harmonic oscillator ground state and the availability of linear and quadratic operators that enable us to prepare the logical input state $|\Psi_0\rangle$. Additionally, the operators R and $\mathsf{R}^\dagger$ identified in Fig. 1 are the easily implementable continuous Fourier transform and its inverse. The oracle information is encoded in the logical state by the unitary operator [17]

$$\mathsf{U}_f = \begin{pmatrix} (-1)^{z_1} & 0 & \cdots & 0 \\ 0 & (-1)^{z_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & (-1)^{z_N} \end{pmatrix}, \tag{14}$$

where the z_i are the bits of the unknown string given in oracle decision problem Definition 1.

Mapping this algorithm to the finite-dimensional, continuously-parameterized coherent spin system must first deal with the step that takes the ground state of the spin system to the logical input state $|\Psi_0\rangle$. This first step also employs physically accessible, linear spin rotation and quadratic spin squeezing.

III. THE SPIN SYSTEM MODEL

The method of generalized coherent states has been successfully used to describe a number of diverse physical phenomena including quantum optics, atom-light interactions, and superfluidity [23]. Here we make use of coherent spin states [24, 25] in creating an alternative model of continuous variable quantum computation. Just as squeezing is beneficial in continuous variable quantum computing using the harmonic oscillator, we make use of spin squeezing here [22]. We use the optimally squeezed spin state [22] as input to our algorithm and show that it can be approximated by a superposition of two discrete states with constant error independent of the size of the Hilbert Space.

A. Coherent Spin States

Our spin system is a collection of $2S$ elementary 1/2 spins. $2S$ is thus an odd integer, and we choose $2S + 1 = N$ so that $N = 2^n$-bit strings may be naturally represented. We refer this as an S-spin system [22].

The system dynamics are determined by the Hamiltonian, which is expressed as a polynomial of su(2) algebraic elements. These algebraic elements are Pauli spin operators in the spin-1/2 single-particle case. For higher even dimensions, we use notation similar to [22] with operators $\hat{\mathsf{S}}_i$, $\hat{\mathsf{S}}_j$ and $\hat{\mathsf{S}}_k$ and i, j, k denoting the components of any three orthogonal directions, such that

$$\left[\hat{\mathsf{S}}_i, \hat{\mathsf{S}}_j\right] = \mathrm{i}\hat{\mathsf{S}}_k, \tag{15}$$

and

$$\Delta\hat{\mathsf{S}}_i^2 \Delta\hat{\mathsf{S}}_j^2 \geq \frac{1}{4}\left\langle \hat{\mathsf{S}}_k \right\rangle^2, \tag{16}$$

and cyclic permutations.

The spin system is oriented in the usual way. With

$$m \in \{-s, -s+1, -s+2, \ldots, s\}, \tag{17}$$

the spin kets $|m\rangle_s$ are eigenstates of $\hat{\mathsf{S}}_z$ and S^2 satisfying

$$\hat{\mathsf{S}}_z |m\rangle_s = m |m\rangle_s, \tag{18}$$

and

$$\mathsf{S}^2 |m\rangle_s = s(s+1) |m\rangle_s, \tag{19}$$

where $\mathsf{S}^2 = \hat{\mathsf{S}}_x^2 + \hat{\mathsf{S}}_y^2 + \hat{\mathsf{S}}_z^2$. The ladder operators are $\hat{\mathsf{S}}_\pm = \hat{\mathsf{S}}_x \pm \mathrm{i}\hat{\mathsf{S}}_y$, and the action of the lowering operator on the ground state is

$$\hat{\mathsf{S}}_- |-s\rangle_s = 0. \tag{20}$$

We use the discrete spin states to construct the continuously parameterized coherent spin states.

The harmonic-oscillator coherent states are *translations* of the oscillator ground state [16]. Analogously, the coherent spin states are *rotations* of the spin-system ground state [22–24]. Individual spin states are often referred to in the literature [23, 24] as Dicke states analogous to photon number states, and the coherent spin states are referred to as Bloch states analogous to Glauber states.

The coherent spin state, $|\theta, \phi\rangle_s$ with $\theta, \phi \in \mathbb{R}$, is [22]:

$$\begin{aligned} |\theta,\phi\rangle_s &= \mathsf{R}_{\theta,\phi} |-s\rangle_s \\ &= \left(1 + \tan^2\frac{\theta}{2}\right)^{-s} \times \\ &\quad \sum_{k=0}^{2s} \binom{2s}{k}^{\frac{1}{2}} \left(e^{\mathrm{i}\phi}\tan\frac{\theta}{2}\right)^k |s-k\rangle_s . \end{aligned} \tag{21}$$

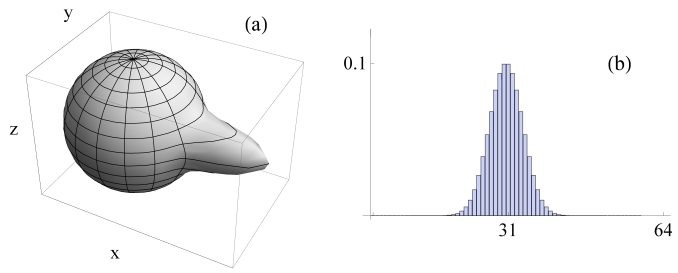

FIG. 2: (a) Spherical Q-function of the state given by Eq. (22) for $s = \frac{63}{2}$, and (b) Plot of the respective Dicke-state probability distribution.

The coherent spin state of most interest is

$$|\pi/2, 0\rangle_s = 2^{-s} \sum_{k=0}^{2s} \binom{2s}{k}^{\frac{1}{2}} |s-k\rangle_s , \tag{22}$$

which has a Dicke-state amplitude spectrum whose squared magnitude is the binomial probability distribution with $p = q = 1/2$ shown in Fig. 2b.

Quasi-probability distributions [23] are a useful means of visualizing spin states. We choose to use Q-functions [23] as coherent-state representations. The spherical plots of these distributions provide good intuition as to the orientation and the isotropic or anisotropic distribution of uncertainties, but they are not used to actually calculate uncertainties, which is performed using Eq. (16).

For the arbitrary coherent spin state represented as $|\Psi\rangle = \sum_{k=0}^{2s} \alpha_k |k\rangle$, we express the spherical Q-function [16] as

$$Q(\theta,\phi) = \sum_{k=0}^{2s} \binom{2s}{k}^{\frac{1}{2}} \sin(\theta/2)^k \cos(\theta/2)^{2s-k} \alpha_k e^{\mathrm{i}k\phi}. \tag{23}$$

In Fig. 2, we plot the spherical Q-function and the probability distribution of the discrete spin state for the state given in Eq. (22). Note that this coherent spin state appears as an 'equatorial' state with isotropic uncertainty distribution when represented this way.

B. Squeezed Spin States

Coherent spin states can be squeezed [22]. Whereas the Glauber states can be squeezed to an arbitrary degree, spin states can only be squeezed to the Heisenberg limit of 1/2 [22]. We wish to exploit the squeezed state with the minimal achievable variance in our algorithm. In the following, we formulate expressions for this optimally squeezed spin state and show that it can be approximated well by a superposition of two spin states.

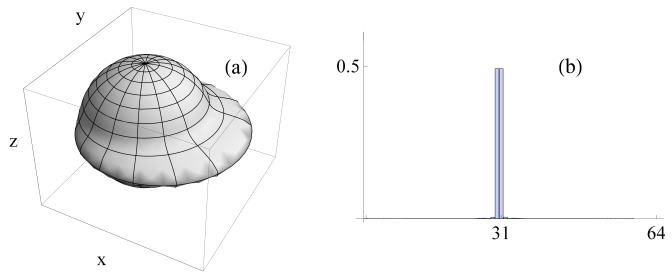

FIG. 3: (a) Spherical Q-function of the squeezed state given by Eq. (27) for $s = \frac{63}{2}$, and (b) Plot of the respective Dicke-state probability distribution.

We employ two-axis counter-twisting [22] to define the squeezing operator

$$\mathsf{S}_\mu = e^{\mathrm{i}\frac{\pi}{4}\hat{\mathsf{S}}_\mathrm{x}} e^{\mathrm{i}\mu\left(\hat{\mathsf{S}}_\mathrm{z}^2 - \hat{\mathsf{S}}_\mathrm{y}^2\right)}, \tag{24}$$

where μ is the squeezing parameter [22]. The rotation operator $e^{\mathrm{i}\frac{\pi}{4}\hat{\mathsf{S}}_\mathrm{x}}$ orients the resulting anisotropic uncertainty distribution in the y, z directions.

Applying the operator S_μ to

$$|\Psi\rangle = |\pi/2, 0\rangle_s \tag{25}$$

allows us to reduce the variance $\Delta\hat{\mathsf{S}}_z^2$ at the expense of enchancing the variance $\Delta\hat{\mathsf{S}}_y^2$. The reduced variance may be expressed as

$$V_- = \langle\hat{\mathsf{S}}_z^2\rangle = \langle\Psi|\,\mathsf{S}_\mu^\dagger\hat{\mathsf{S}}_z^2\mathsf{S}_\mu\,|\Psi\rangle \tag{26}$$

since the first moment $\langle\hat{\mathsf{S}}_z\rangle = 0$. In Fig. 3a, we plot the quasi-probability distribution of a squeezed spin state. The reduced variance of the squeezed state in the z direction and increased variance in the y direction is evident.

The minimum value of the reduced variance V_- asymptotically approaches $1/2$ with increasing s [22]. We refer to the optimal value of the squeezing parameter at this minimum as μ_opt. For $\mu > \mu_\mathrm{opt}$, the distribution variance increases and the distribution quasi-probability distribution becomes becomes skewed [22]. It can shown be that $\mu_\mathrm{opt} \to \frac{1}{s}$ as $s \to \infty$. This limit is understandable since the variance of a binomial distribution with $p = q = 1/2$ is $N/4$, and squeezing simply has the effect of removing the distribution variance of the dependency on $N = 2s + 1$.

We express the optimally-squeezed spin state as

$$\begin{aligned}\left|\Phi^{(N)}\right\rangle &= |\pi/2, 0, \mu_\mathrm{opt}\rangle_s \\ &= \mathsf{S}_{\mu_\mathrm{opt}}\,|\Psi\rangle\,,\end{aligned} \tag{27}$$

with $|\Psi\rangle$ defined in Eq. (25). In Fig. 3b, we plot the Dicke-state probability distribution of the optimally squeezed state. It is evident that this state approximates the superposition of two spin states. We wish to provide a bound on how well approximated the squeezed state is by a two-component superposition.

Analysis of the variance of the squeezed state's probability distribution is facilitated using the qudit representation rather than the spin sate representation. We thus represent this N-dimensional squeezed state in terms of the qudits $|i\rangle$ as

$$\left|\Phi^{(N)}\right\rangle = \sum_{i=0}^{N-1}\alpha_i|i\rangle. \tag{28}$$

The probability distribution associated with $\left|\Phi^{(N)}\right\rangle$ may be represented as the set

$$\mathcal{P}^{(N)} = \{|\alpha_0|^2, \ldots, |\alpha_i|^2, \ldots, |\alpha_{N-1}|^2\}, \tag{29}$$

with individual probabilities $\mathcal{P}_i^{(N)} = |\alpha_i|^2$. We note that the squeezed state is symmetric about the centre, and thus the two central states have

$$\mathcal{P}_{(N/2-1)}^{(N)} = \mathcal{P}_{(N/2)}^{(N)} = P_c^{(N)}, \tag{30}$$

and thereby form the principle components of the probability distribution of optimally squeezed states.

For $s > \frac{3}{2}$, the expression for the reduced variance given by Eq. (26) requires solving eigenvalue problems of degree greater than eight and is no longer analytic, and we must resort to numerical analysis. For $s = 3/2$ and $N = 4$ the expression for the reduced variance given by Eq. (26) is analytic, and $\mu_\mathrm{opt} = \frac{\pi}{6\sqrt{3}}$. We can thus represent the optimal squeezed state as

$$\left|\Phi^{(4)}\right\rangle = e^{\mathrm{i}\phi}\left(0|0\rangle + \frac{1}{\sqrt{2}}|1\rangle + \frac{1}{\sqrt{2}}|2\rangle + 0|3\rangle\right), \tag{31}$$

where $e^{\mathrm{i}\phi}$ is a global phase picked up by the action of S_μ. The associated probability distribution is

$$\mathcal{P}^{(4)} = \{0, 1/2, 1/2, 0\}. \tag{32}$$

For this case we achieve what we refer to as 'perfect' squeezing, where 'perfect' means that the two central components have probability equal to a half, and the probability of the other two components is zero.

However, this four component distribution has a variance of only a quarter, where the distribution variance is expressed as

$$\mathrm{Var}\left[\mathcal{P}^{(N)}\right] = \sum_{i=0}^{N-1} i^2\,|\alpha_i|^2 - \left(\sum_{i=0}^{N-1} i\,|\alpha_i|^2\right)^2. \tag{33}$$

Indeed for all N if $\mathcal{P}_c^{(N)} = 1/2$ then,

$$\begin{aligned}\mathrm{Var}\left[\mathcal{P}^{(N)}\right] =& \frac{1}{2}\left((N/2-1)^2 + (N/2)^2\right) - \frac{1}{4}(N-1)^2 \\ =& \frac{1}{4}.\end{aligned} \tag{34}$$

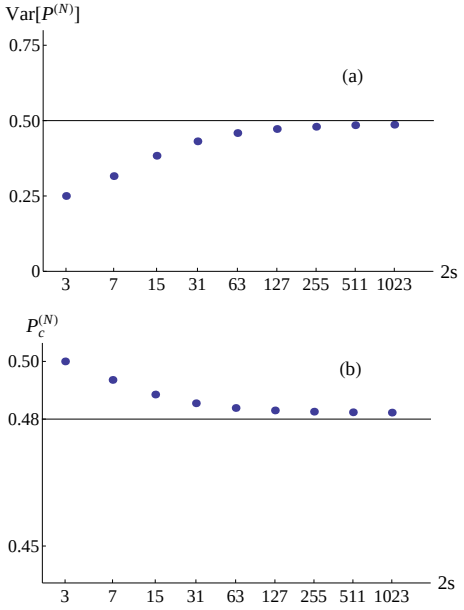

FIG. 4: (a) Calculated value of the reduced variance of the probability distribution given by Eq. (26) approaches 1/2 with increasing s as predicted [22]. (b) Calculated value of the probability of the two central components given by Eq. (30) is bounded by the constant given by Eq. (37).

Since the distribution variance approaches 1/2 as $N = 2s+1$ approaches infinity, perfect squeezing in the sense we have defined is not possible. We use the variance equals 1/2 as a means to bound $\mathcal{P}_c^{(N)}$ defined in Eq. (30). In Fig. 4a, we plot the calculated values of the reduced variance given by Eqs. (26) and (33) as a function of s from $s = 3/2$ to $s = 1023/2$, where we observe that the variance approaches $V = 1/2$ as predicted. In order to bound the limiting value of the two central components $\mathcal{P}_c^{(N)}$, we bound the 'tails' of the probability distribution $\mathcal{P}^{(N)}$.

In Fig. 5, we plot histograms calculated from the squeezed distribution, $\mathcal{P}^{(N)}$, for several values of s, where we have scaled the ordinate to reveal the structure of the tail components. We see that the components immediately adjacent to the central components have

$$\mathcal{P}^{(N)}_{N/2+1} = \mathcal{P}^{(N)}_{N/2-2} \approx 0, \tag{35}$$

and further outlying terms tail off in an exponential-like fashion. We thus introduce the following bounding probability distribution

$$\mathcal{P}^{(N)}_{\mathcal{B}} = \left\{0, \ldots, 0, \frac{\epsilon}{3}, \frac{2\epsilon}{3}, 0, \frac{1}{2} - \epsilon, \right. \tag{36}$$
$$\left. \frac{1}{2} - \epsilon, 0, \frac{2\epsilon}{3}, \frac{\epsilon}{3}, 0, \ldots, 0\right\},$$

in order to calculate a bound on the two central components of the distribution.

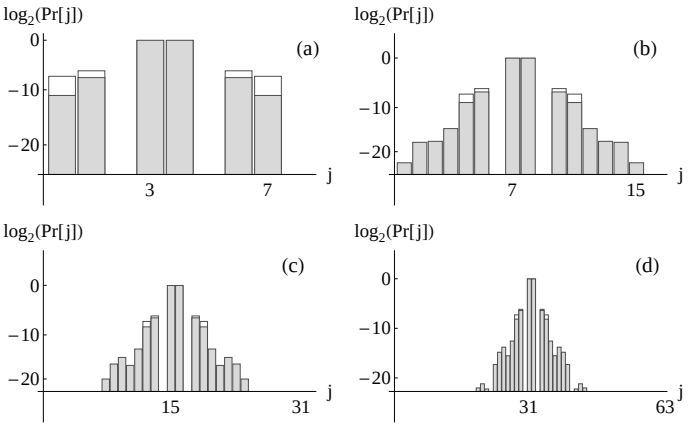

FIG. 5: Histograms of the probability distribution $\mathcal{P}^{(N)}$ for (a) $s = 7/2$, (b) $s = 15/2$, (c) $s = 31/2$ and (d) $s = 63/2$ with a logarithmic scale for the ordinate. The bounding distribution given by Eqs. (36) and (37) is overlayed on each of the histograms.

Solving Var $\left[\mathcal{P}^{(N)}_{\mathcal{B}}\right] = 1/2$ for ϵ gives the probability of the two central components

$$\mathcal{P}^{(N)}_{\mathcal{B}_c} = \frac{1}{2} - \epsilon \approx 0.484. \tag{37}$$

In Fig. 4b, we plot the calculated values of $\mathcal{P}_c^{(N)}$, where we note that it goes from 1/2 at $s = 3/2$ and asymptotically approaches the constant bounded from below by Eq. (37). The bounding distribution is also overlayed on the histograms presented in Fig. 5.

Since greater than 98% of the probability is manifest in the two central components, we approximate the optimally squeezed input state by the superposition of two states

$$|\Psi_0\rangle = \frac{1}{\sqrt{2}}\left(\left|\frac{1}{2}\right\rangle_s + \left|-\frac{1}{2}\right\rangle_s\right), \tag{38}$$

and we can leave the spin system model behind because the ideal state given in Eq. (38) can be used as input on any quantum computer. We emphasize that the idea to use it as input to the algorithm give in Fig. 1 has been inspired through the analysis of the continuously parameterized finite-dimensional Hilbert space of the s-spin system.

IV. EFFICIENT ALGORITHM FOR THE CLOSE HADAMARD PROBLEM

An important principle in quantum information processing is the solving of problems with increased efficiency compared to classical information processing. Efficiency can be measured in terms of a problem's query complexity, and in this section we present two claims quantifying the query complexity required to solve the close Hadamard problem in the quantum setting.

For a quantum algorithm employing the quantum circuit in Fig. 1 with $\mathsf{R} = \mathsf{R}^\dagger = \mathsf{H}^{\otimes n}$, we state the number of oracle queries required to solve the restricted and the unrestricted close Hadamard problem defined in Problem 1 and Problem 2 respectively. We prove these claims through the introduction and proof of three Lemmas. We follow this with a discussion of the query complexity of classical algorithms.

With the idealized input state simplified to

$$|\Psi_0\rangle = \left|\frac{1}{2}\right\rangle_s + \left|-\frac{1}{2}\right\rangle_s, \tag{39}$$

where we have suppressed the normalization factor $\frac{1}{\sqrt{2}}$ in Eq. (38), the action of the algorithm on the input state is expressed as

$$|\Psi_3\rangle = \mathsf{H}^{\otimes n}\mathsf{U}_z\mathsf{H}^{\otimes n}\,|\Psi_0\rangle\,. \tag{40}$$

The N-bit string z represents the function f. We show that the algorithm efficiently solves both versions of the close Hadamard problem.

Claim 1. *The restricted close Hadamard problem can be solved with certainty in a single oracle query using the quantum circuit given in Fig. 1 and the idealized input state given by Eq. (39).*

Claim 2. *The un-restricted close Hadamard problem can be solved with arbitrarily small error probability in a constant number of oracle queries using the quantum circuit given in Fig. 1 and the idealized input state given by Eq. (39).*

A. Algorithm Response to the Hadamard Codewords

A key feature of the input state is that it is a symmetric superposition of two basis states. When Hadamard codewords are encoded into the oracle, the action of the algorithm preserves the symmetric superposition. This preservation is demonstrated in Fig. 6. We thus prove the following Lemma is true.

Lemma 1. *Given the input* $|\Psi_0\rangle = \left|\frac{1}{2}\right\rangle_s + \left|-\frac{1}{2}\right\rangle_s$ *to the circuit shown in Fig. 1 and the oracle encoded with one of the Hadamard codewords* $z = W_j^{(N)}$ *for* $N = 2s+1$ *and* $0 \le j < \frac{N}{2}$*, the output state is another superposition of spin states* $|\Psi_3\rangle = \left|\frac{1}{2}+j\right\rangle_s + \left|-\frac{1}{2}-j\right\rangle_s$.

Proof. In order to simplify notation in the following, we suppress the superscript N in $W_j^{(N)}$. With W defined as the set of Hadamard codewords given by Eq. (2), the pair $(W, \oplus)$ forms a group under addition modulo two [27]. In particular, the identity element is W_0, and each element is its own inverse since

$$W_j \oplus W_j = W_0. \tag{41}$$

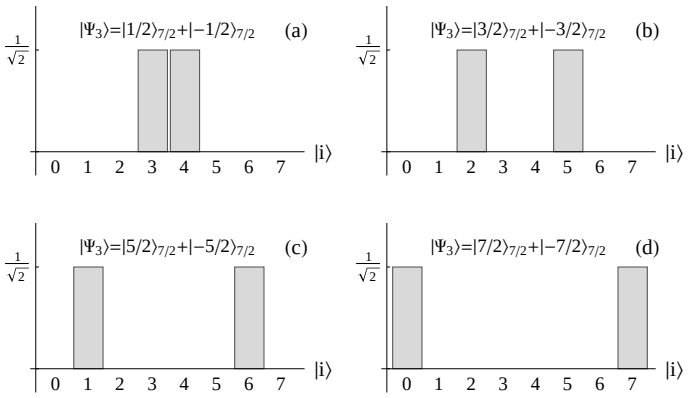

FIG. 6: For the example of $s = 7/2$, $N = 8$, the output state given by Eq. (43) remains a symmetric superposition of two states for the Hadamard codewords: (a) $W_0^{(8)}$, (b)$W_1^{(8)}$, (c) $W_2^{(8)}$, and (d) $W_3^{(8)}$.

It follows from the group property that the addition of any two codewords is another codeword. For the Hadamard codeword pairs W_j and W_{N-1-j}, it can be readily shown that

$$W_j \oplus W_{N-1-j} = W_{N-1} \tag{42}$$

for all $j \in \mathbb{Z}_N$.

With some algebraic manipulation, the state $|\Psi_3\rangle$ may be expressed as

$$|\Psi_3\rangle = \frac{1}{N}\sum_{y=0}^{N-1}\left(\sum_{x=0}^{N-1}\alpha_{x,y}\right)|y\rangle\,. \tag{43}$$

We use the qudit representation $|y\rangle$ rather than the spin state representation $|m\rangle_s$. We translate back to spin state representation as the last step.

The symbol

$$\alpha_{x,y} = (-1)^{\left(z\oplus W_{y+N/2}\right)_x} + (-1)^{\left(z\oplus W_{N/2-(y+1)}\right)_x}, \tag{44}$$

where $z = W_j$ is the string encoded in the oracle, and the symbol x represents the x^{th} bit of the N-bit strings. Note that the sums $y+N/2$ and $N/2-(y+1)$ in Eq. (44) are modulo N sums.

The Hadamard codewords are balanced with the exception of W_0, which is constant. For $j \neq k$, this allows us to write

$$0 = \sum_{x=0}^{N-1}(-1)^{(W_j\oplus W_k)_x}, \tag{45}$$

and for $j = k$,

$$N = \sum_{x=0}^{N-1}(-1)^{(W_j\oplus W_j)_x}, \tag{46}$$

where we have used the group inverse relation given in Eq. (41). Using this result, we see that a non-zero sum of $\alpha_{x,y}$ in Eq. (43) occurs exactly twice when $y = (N/2+j) \mod N$ and when $y = (N/2-1-j) \mod N$.

In the qudit representation, the output state is thus expressed

$$|\Psi_3\rangle = |N/2-1-j\rangle + |N/2+j\rangle\,, \tag{47}$$

where qudit indices are understood to be modulo N. For $0 \le j < N/2$, this translates back to the spin basis as

$$|\Psi_3\rangle = |-1/2-j\rangle_s + |1/2+j\rangle_s\,, \tag{48}$$

thus completing the proof of Lemma 1. □

We now show that the superposition of two states is also preserved for codewords with restricted errors.

Lemma 2. *Given the input $|\Psi_0\rangle = \left|\frac{1}{2}\right\rangle_s + \left|-\frac{1}{2}\right\rangle_s$ to the circuit shown in Fig. 1 and the oracle encoded with $z \in \tilde{\Xi}_j^{(N)}$ given by Eq. (12), which is a codeword having restricted errors, and with $0 \le j < \frac{N}{2}$, the output state is another superposition of spin states $|\Psi_3\rangle = \left|\frac{1}{2}+j\right\rangle_s + \left|-\frac{1}{2}-j\right\rangle_s$.*

Proof. Observe that the form of Eq. (44) allows for cancelling of errors. Under certain conditions if an error occurs at bit position x, the effect on the left-hand side of the plus sign is cancelled by the opposite effect on the right-hand side. Consider the x^{th} bit error in Eq. (44), where we have cancellation

$$0 = (-1)^{\left(z \oplus W_{y+N/2}\right)_x} + (-1)^{\left(z \oplus W_{N/2-(y+1)}\right)_x}. \tag{49}$$

This identity implies that

$$\begin{aligned} 1 &= \left(W_{y+N/2} \oplus W_{N/2-(y+1)}\right)_x \\ &= (W_{N-1})_x, \end{aligned} \tag{50}$$

where we have used the result expressed in Eq. (42). This is exactly the same as the requirement to be a member of set $\tilde{\Xi}_j^{(N)}$ defined in Eq. (12). Under this condition, the result of Lemma 1 holds and $|\Psi_3\rangle = \left|\frac{1}{2}+j\right\rangle_s + \left|-\frac{1}{2}-j\right\rangle_s$. □

We now show that the perfect superposition of two states is no longer preserved for codewords having unrestricted errors. The effect of errors that are not of the restricted type is to degrade the superposition by distributing amplitude evenly across all other states. However as long as the number of these errors is less than $N/16$, it is still possible to efficiently identify the desired state.

Lemma 3. *Given the input $|\Psi_0\rangle = \left|\frac{1}{2}\right\rangle_s + \left|-\frac{1}{2}\right\rangle_s$ to the circuit shown in Fig. 1 and the oracle encoded with $z \in \Xi_j^{(N)}$ given by Eq. (7), which is a codeword having less than $N/16$ unrestricted errors, the desired state can be identified with success probability of at least $\frac{9}{16}$.*

Proof. Let $V_j \in \Xi_{j,1}^{(N)}$ be a Hadamard codeword with a single unrestricted error. We have already shown that if the error is of the restricted type, two-component superpositions are preserved. If the the error is not a restricted error, we have no error cancellation, so the single bit-error breaks the balanced and constant sums defined by Eqs. (45) and (46), respectively. For $j \ne k$ this gives

$$2 = \sum_{x=0}^{N-1} (-1)^{(W_j \oplus V_k)_x}, \tag{51}$$

and for $j = k$,

$$N-2 = \sum_{x=0}^{N-1} (-1)^{(W_j \oplus V_j)_x}. \tag{52}$$

As the input state is a two-component superposition, the above sums result in all the amplitudes of the output state either acquiring or losing an amount of amplitude proportional to four — two from the amount in the balanced or constant sums given in Eqs. (51) and (52) and two from the effect of there being two components in the input state.

Thus, we express the output state for the worst case of a single unrestricted error as

$$\begin{aligned} |\Psi_3\rangle =& \frac{1}{\sqrt{2}}\left(1-\frac{4}{N}\right)\left(\left|\frac{1}{2}+j\right\rangle_s + \left|-\frac{1}{2}-j\right\rangle_s\right) \\ &+ \frac{4}{\sqrt{2}N} \sum_{\substack{k=-s-1/2 \\ k \ne \pm j}}^{k=s-1/2} \pm \left|\frac{1}{2}+k\right\rangle_s . \end{aligned} \tag{53}$$

For the worst case of l unrestricted errors, where no errors are of the restricted type, the principle components have amplitude

$$\alpha = \frac{1}{\sqrt{2}}\left(1-\frac{4l}{N}\right), \tag{54}$$

and the amplitude of the next largest component is

$$\beta = \frac{4l}{\sqrt{2}N}. \tag{55}$$

The amplitude reduction of the principle components by an amount directly proportional to the number of errors results from the constant sum given by Eq. (52) being reduced by double the number of errors. However, the balanced sums are variable since errors can cancel. The worst case occurs when the errors are 'in phase' resulting in the amplitude of the next-largest component being proportional to the number of errors. The effect of codewords with unrestricted errors on the input superposition is presented in Fig. 7.

The probability of the two central components is

$$|\alpha|^2 \ge \frac{1}{2}\left(1-\frac{8l}{N}+\frac{16l^2}{N^2}\right). \tag{56}$$

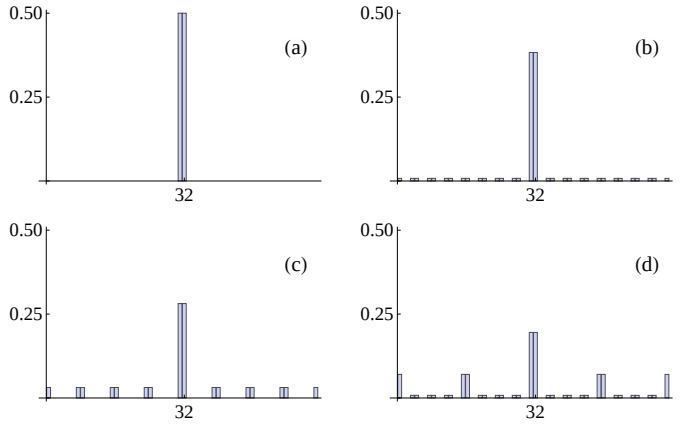

FIG. 7: For $N = 64$, the effect of l unrestricted errors, where none of the l errors are of the restricted type, on the probability of the central components is demonstrated for (a) $l = 0$, (b) $l = 2$, (c) $l = 4$, and (d) $l = 6$. Fig. 7(c) corresponds to the case that $l = N/16$.

The equality holds for the worst case where none of the errors are of the restricted type. If $l = N/16$, then $|\alpha|^2 \geq \frac{1}{2}\left(\frac{9}{16}\right)$. The amplitudes of the two central states can be combined into a single state with amplitude $\sqrt{2}\alpha$ by an appropriate unitary operation. Since l is less than $N/16$, the desired state can be identified with probability $2|\alpha|^2$, which is at least $\frac{9}{16}$. □

B. Solution of the Close Hadamard Problem

We now use results of Lemmas 1, 2 and 3 to show that Claims 1 and 2 are true.

Proof of Claim 1:

By Lemmas 1 and 2, $|\Psi_3\rangle = \left|\frac{1}{2}+j\right\rangle_s + \left|-\frac{1}{2}-j\right\rangle_s$ for $z \in \tilde{\Xi}_j^{(N)}$. Immediately prior to the measurement step, we require a unitary operator $\mathsf{U}_{2\mapsto 1}$ that maps this superposition of two states into a single basis state such that

$$\mathsf{U}_{2\mapsto 1}|\Psi_3\rangle = \left|\frac{1}{2}+j\right\rangle_s. \tag{57}$$

Since we know that the unknown string z is either in set $\tilde{\Xi}_{N/2-1}^{(N)}$ or in $\tilde{\Xi}_k^{(N)}$, we wish to measure the outcome of the qudit $|s\rangle_s$ in the spin basis. We define the projection operator [31]

$$M_s = |s\rangle_s \langle s|, \tag{58}$$

and outcome probability is

$$\Pr[s] = \left\langle \frac{1}{2}+j\right|_s M_s \left|\frac{1}{2}+j\right\rangle_s. \tag{59}$$

If $j = N/2-1$, then $\Pr[s] = 1$ and $z \in A$, and if $j \neq N/2-1$, then $\Pr[s] = 0$ and $z \in B$. Thus, the restricted close Hadamard problem is solved with certainty in a single oracle query. □

Proof of Claim 2:

By Lemmas 1 and 2, $|\Psi_3\rangle = \left|\frac{1}{2}+j\right\rangle_s + \left|-\frac{1}{2}-j\right\rangle_s$ for $z \in \tilde{\Xi}_j^{(N)}$. By Lemma 3, the effect of including l unrestricted bit errors on the output state may be expressed as

$$\begin{aligned}|\Psi_3\rangle =& \alpha\left(\left|\frac{1}{2}+j\right\rangle_s + \left|-\frac{1}{2}-j\right\rangle_s\right) \\ &+ \beta\sum_\kappa \pm\left|\frac{1}{2}+k\right\rangle_s + \gamma\sum_\lambda \pm\left|\frac{1}{2}+k\right\rangle_s,\end{aligned} \tag{60}$$

where the symbols α and β are given by Eqs. (54) and (55) respectively, and $|\gamma| < |\beta|$. Note that $\kappa + \lambda = N-2$, so that all N possible states are accounted for, but the specific value of γ, κ and λ are dependent on N and l. The outcome probabilities of measuring the state $|s\rangle_s$ are thus

$$\Pr[s] = \left\langle \frac{1}{2}+j\right|_s M_s \left|\frac{1}{2}+j\right\rangle_s. \tag{61}$$

If $j = N/2-1$, then $\Pr[s] > |\alpha|^2$, and if $j \neq N/2-1$, then $\Pr[s] < |\beta|^2$. Assuming that the number of unrestricted errors l is less than $N/16$, then an error of $O(e^{-q})$ can be achieved by making $O(q)$ repetitions of the algorithm [17]. Thus, the unrestricted close Hadamard problem is solved with arbitrarily small error probability in a constant number of queries. □

C. Classical Algorithm

In this subsection we compare the performance of any classical algorithm to the performance of the quantum algorithm.

Claim 3. *Any classical deterministic algorithm requires $\Omega(n)$ oracle queries of the bit positions to solve the close Hadamard problem with certainty,* even *if there are no bit errors. A randomized algorithm with bounded error probability also requires $\Omega(n)$ queries,* even *if there are no bit errors.*

Claim 3 follows from information theoretical considerations. The goal of the classical strategy is to determine which of the $N/2$ Hadamard codewords is loaded into the oracle. The number of possible solutions is then initially $\Omega(2^n)$. Whenever a classical strategy performs a query, it can eliminate at most half of the remaining possible solutions, even if there are no errors. To reduce the number of possible solutions to a single solution, the classical strat-

egy therefore requires at least $\Omega(n)$ queries[1]. The lower bound also holds when the strings loaded into the oracle are Hadamard codewords with errors.

In the next session we discuss how changing the unitary operators R and $\mathsf{R}^\dagger$ in the algorithm shown in Fig. 1 changes the oracle decision problem that can be solved.

V. ALTERNATIVE ALGORITHM

The continuously-parameterized, finite-dimensional Hilbert space of the spin system inspired an efficient algorithm for the solution of the close Hadamard problem. The group structure of the Hadamard codewords is implicit in the use of Hadamard operators in the quantum algorithm. We now show that this computation model can inspire other algorithms. Other unitary operators can be employed in the quantum circuit shown in Fig. 1. The discrete Fourier transform [31] is an obvious alternative. We provide a sketch of how the Fourier transform changes the group structure of the codewords and point to the need for further exploration of problems that could benefit from this computational model.

We replace the operators R and $\mathsf{R}^\dagger$ in Fig. 1 with the discrete Fourier transform F and $\mathsf{F}^\dagger$. The matrix representation of the discrete Fourier transform is expressed as

$$\mathsf{F}^{(N)} = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega & \cdots & \omega^{N-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{(N-1)} & \cdots & \omega^{(N-1)(N-1)} \end{pmatrix}, \quad (62)$$

where $\omega = e^{\frac{\mathrm{i}\pi}{N}}$ [31].

In our analysis of the F-based algorithm, we adopt a similar approach to that taken for the H-based algorithm and define the 'Fourier codewords' as

$$\mathsf{T}^{(N)} = \log_{(-1)} \left[\sqrt{N} \mathsf{F}^{(N)} \right]. \quad (63)$$

Similar to the Hadamard codewords, the j^{th} Fourier codeword is the j^{th} row of the matrix $\mathsf{T}^{(N)}$. As an example, we express the $N = 8$ matrix as

$$\mathsf{T}^{(8)} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{4} & \frac{1}{2} & \frac{3}{4} & 1 & -\frac{3}{4} & -\frac{1}{2} & -\frac{1}{4} \\ 0 & \frac{1}{2} & 1 & -\frac{1}{2} & 0 & \frac{1}{2} & 1 & -\frac{1}{2} \\ 0 & \frac{3}{4} & -\frac{1}{2} & \frac{1}{4} & 1 & -\frac{1}{4} & \frac{1}{2} & -\frac{3}{4} \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & -\frac{3}{4} & \frac{1}{2} & -\frac{1}{4} & 1 & \frac{1}{4} & -\frac{1}{2} & \frac{3}{4} \\ 0 & -\frac{1}{2} & 1 & \frac{1}{2} & 0 & -\frac{1}{2} & 1 & \frac{1}{2} \\ 0 & -\frac{1}{4} & -\frac{1}{2} & -\frac{3}{4} & 1 & \frac{3}{4} & \frac{1}{2} & \frac{1}{4} \end{pmatrix}, \quad (64)$$

with $T_4^{(8)} = 01010101$. We see that the Fourier codewords are not bit strings but rather can be thought of as fractional bits. These fractional bits can still be encoded into the oracle function U_z given in Eq. (14).

We now define what we term the *simple Fourier codeword* oracle decision problem and show that it can be solved in a single query using the modified algorithm. Note that we have structured this problem along the same lines as the close Hadamard problem with no errors.

Problem 3. *Given the string $\check{A} = T_{N/2-1}^{(N)}$ and a set of strings $\check{B} = T_k^{(N)}$, with $k \in \{\mathbb{Z}_N \mid k \neq N/2-1\}$ and a string z randomly selected with uniform distribution μ such that $z \in_\mu \check{C} = \check{A} \cup \check{B}$, the* ***Simple Fourier Codeword*** *problem is to determine if $z \in \check{A}$ or $z \in \check{B}$ with the fewest oracle queries.*

The action of the algorithm on the input state is expressed as

$$|\Psi_3\rangle = \mathsf{F}^{\dagger(N)} \mathsf{U}_z \mathsf{F}^{(N)} \left(\left| \frac{1}{2} \right\rangle_s + \left| -\frac{1}{2} \right\rangle_s \right). \quad (65)$$

For $z = T_j^{(N)}$ and $j \in 0, 1, \ldots, N-1$, the output state can be shown to be

$$|\Psi_3\rangle = \left| \frac{1}{2} + j \right\rangle_s + \left| -\frac{1}{2} + j \right\rangle_s, \quad (66)$$

where $\frac{1}{2} + j$ and $-\frac{1}{2} + j$ are modulo s sums in the sense that $\left|\frac{1}{2} + \frac{N}{2}\right\rangle = |-s\rangle$.

We apply $U_{2 \mapsto 1}$ given in Eq. (57) to the state $|\Psi_3\rangle$ given in Eq. (66). Measuring the qudit $|s\rangle_s$ in the spin basis with the measurement operator M_s given in Eq. (58), distinguishes whether the encoded string is in set $\check{A}$ or set $\check{B}$ thereby solving the simple Fourier codeword problem in a single query.

The result given by Eq. (66) is achieved by exploiting group properties similar to those expressed in Eqs. (41) and (42) for the Hadamard codewords. The columns of $\mathsf{F}^{(N)}$ represent the *multiplicative* cyclic group of order N, where the generator is the first non-trivial column of $\mathsf{F}^{(N)}$. The matrix of codewords $\mathsf{T}^{(N)}$ represents the *additive* cyclic group of order N as a result of taking the logarithm of $\mathsf{F}^{(N)}$.

Each element of the group has the inverse relation

$$T_j + T_{N-j} = T_0, \quad (67)$$

and each codeword also obeys the sum relation

$$T_j + T_{N/2-j} = T_{N/2}, \quad (68)$$

where $N - j$ and $N/2 - j$ are understood to be modulo N sums. In Fig. 8 we clearly see that, unlike, the Hadamard codewords that preserve the superposition of two symmetric states, the Fourier codewords preserve the superposition of two adjacent states.

[1] See for example paragraph 6.1 in [32] for an introduction to information theoretic lower bounds.

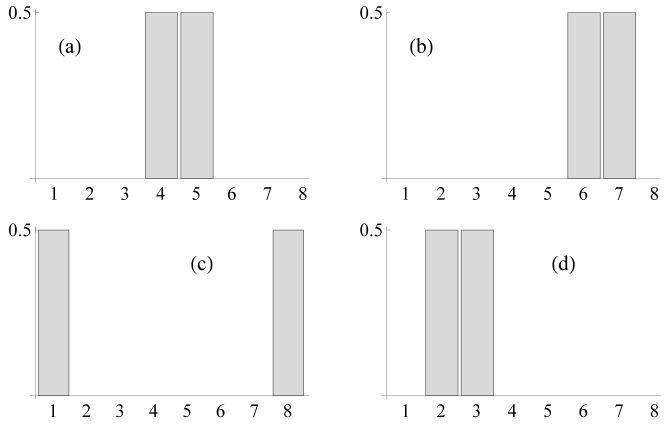

FIG. 8: For $s = 7/2$, the Fourier-based algorithm probability distributions for the states given by Eq. (66) for (a) $j = 0$, (b) $j = 2$ (c) $j = 4$ and (d) $j = 6$. The F-based algorithm preserves the 'adjacency' of the input superposition, whereas the H-based algorithm preserves the 'mirror' symmetry of the input superposition as shown in Fig. 6.

Comparison of the effect of the different operators is interesting. The Hadamard codewords preserve symmetric superpositions, and there are $N/2$ unique symmetric superpositions. The Fourier codewords preserve adjacent superpositions, and there are N unique adjacent superpositions.

The exploration of the structure of error cancellations along the lines of Eq. (50) using the relationship Eq. (68) for the Fourier codewords may lead to new problems that can be efficiently solved using this model of computation. For example, it is natural to apply this error cancellation concept to the simple Fourier codeword oracle decision problem presented in Problem 3 so that the equivalent of Fourier codewords with errors may be included.

VI. CONCLUSIONS

We have shown that the continuously-parameterized coherent spin state representation of a finite-dimensional Hilbert space of elementary 1/2 spins gives us a new continuous variable model of quantum computation. Like continuous variable quantum computation using the states of the harmonic oscillator, this spin system is amenable to physical preparation with linear rotation and quadratic squeezing operators. Unlike the harmonic oscillator case, spin squeezing is Heisenberg limited. We have shown that the optimally-squeezed coherent spin state is well approximated by a superposition of two discrete states.

Using this idealized state as input into a quantum algorithm presented in Fig. 1, which is adapted from the single-mode continuous variable case, we have discovered a new oracle decision problem, which we call the close Hadamard problem. This problem is related to the digital error correction technique of employing Hadamard stings as error-tolerant codewords.

We have shown that the unrestricted version of this problem can be solved in a constant number of queries with arbitrarily small error probability, whereas its classical counterpart requires $\Omega(n)$ queries. More interestingly, we have also shown the restricted version of the problem is solved in a single query with certainty.

The observed speedup, in the restricted case, results from the combination of the group structure of the Hadamard codewords, the employment of the Hadamard operator $\mathsf{H}^{\otimes n}$ as the operator R in Fig. 1 and the use of a symmetric superposition of two basis states as the algorithm input. The tolerance of errors in this case is a direct result of the cancellation of errors that results from this combination.

We have also shown that this algorithm can be generalized. We can change the operator R in Fig. 1 to the discrete Fourier transform, and loading Fourier codewords into the oracle preserves the symmetry of the input state superposition in a manner analogous to the close Hadamard problem. This pairing between operators and the codewords loaded into the oracle offers the promise of discovery of new problems that can be efficiently solved this way.

We conclude that the continuously-parameterized representation of quantum dynamical systems having a finite-dimensional Hilbert space gives us a model of quantum computation that inspires efficient solutions of new problems.

Acknowledgements

We appreciate financial support from the Alberta Ingenuity Fund (AIF), Alberta Innovates Technology Futures (AITF), Canada's Natural Sciences and Engineering Research Council (NSERC), the Canadian Network Centres of Excellence for Mathematics of Information Technology and Complex Systems (MITACS), and the Canadian Institute for Advanced Research (CIFAR).

[1] Benioff, P., "Quantum mechanical models of Turing machines that dissipate no energy," *Phys. Rev. Lett.*, Vol. 48, 1982, pp. 1581–1585. doi:10.1103/PhysRevLett.48.1581.

[2] Feynman, R. P., "Simulating Physics with Computers," *Int. J. Theor. Phys.*, Vol. 21, 1982, pp. 467–488. doi:10.1007/BF02650179.

[3] Deutsch, D., "Quantum theory, the Church-Turing principle and the universal quantum computer," *Proc. R. Soc. Lond. A*, Vol. 400, July 1985, pp. 97–117. doi:10.1098/rspa.1985.0070.

[4] Kielpinski, D., Monroe, C., and Wineland, D. J., "Architecture for a large-scale ion-trap quantum computer," *Nature*, Vol. 417, 2002, pp. 709–711. doi:10.1038/nature00784.

[5] Vandersypen, L. M. K., Steffen, M., Breyta, G., Yannoni, C. S., Sherwood, M. H., and Chuang, I. L., "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance," *Nature*, Vol. 414, 2001, pp. 883–887. doi:10.1038/414883a.

[6] Loss, D. and DiVincenzo, D. P., "Quantum computation with quantum dots," *Phys. Rev.*, Vol. A57, 1998, pp. 120–126. doi:10.1103/PhysRevA.57.120.

[7] Braunstein, S. L. and Pati, A. K., *Quantum Information with Continuous Variables*, Kluwer Academic Publisher, Dordrecht, NL, 2003.

[8] Furusawa, A., Sørensen, J. L., Braunstein, S. L., Fuchs, C. A., Kimble, H. J., and Polzik, E. S., "Unconditional quantum teleportation," *Science*, Vol. 282, 1998, pp. 706–709. doi:10.1126/science.282.5389.706.

[9] Grosshans, F. and Grangier, P., "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.*, Vol. 88, 2002, pp. 057902. doi:10.1103/PhysRevLett.88.057902.

[10] Appel, J., Figueroa, E., Korystov, D., Lobino, M., and Lvovsky, A. I., "Quantum memory for squeezed light," *Phys. Rev. Lett.*, Vol. 100, 2008, pp. 093602. doi:10.1103/PhysRevLett.100.093602.

[11] Akamatsu, D., Yokoi, Y., Arikawa, M., Nagatsuka, S., Tanimura, T., Furusawa, A., and Kozuma, M., "Ultraslow propagation of squeezed vacuum pulses with electromagnetically induced transparency," *Phys. Rev. Lett.*, Vol. 99, 2007, pp. 153602. doi:10.1103/PhysRevLett.99.153602.

[12] Braunstein, S. L., "Error correction for continuous quantum variables," *Phys. Rev. Lett.*, Vol. 80, 1998, pp. 4084–4087. doi:10.1103/PhysRevLett.80.4084.

[13] Eisert, J., Plenio, M. B., and Scheel, S., "Distilling Gaussian states with Gaussian operations is impossible," *Phys. Rev. Lett.*, Vol. 89, 2002, pp. 137903. doi:10.1103/PhysRevLett.89.137903.

[14] Bartlett, S. D. and Sanders, B. C., "Efficient classical simulation of optical quantum information circuits," *Phys. Rev. Lett.*, Vol. 89, 2002, pp. 207903. doi:10.1103/PhysRevLett.89.207903.

[15] Bartlett, S. D., Sanders, B. C., Braunstein, S. L., and Nemoto, K., "Efficient classical simulation of continuous variable quantum information processes," *Phys. Rev. Lett.*, Vol. 88, 2002, pp. 07904. doi:10.1103/PhysRevLett.88.097904.

[16] Leonhardt, U., *Measuring the Quantum State of Light*, Cambridge University Press, Cambridge UK, 1997.

[17] Adcock, M. R. A., Høyer, P., and Sanders, B. C., "Limitations on continuous variable quantum algorithms with Fourier transforms," *New J. Phys.*, Vol. 11, 2009, pp. 103035. doi:10.1088/1367-2630/11/10/103035.

[18] Adcock, M. R. A., Høyer, P., and Sanders, B. C., "Gaussian quantum computation with oracle-decision problems," in preparation.

[19] Cerf, N., Høyer, P., Magnin, L., and Sanders, B. C., "Quantum algorithms with continuous variables for black box problems," *3rd International Workshop on Physics and Computation (P&C 2010)*, 2010.

[20] Deutsch, D., "Quantum computational networks," *Proc. R. Soc. Lond. A*, Vol. 425, September 1989, pp. 73–90. doi:10.1098/rspa.1989.0099.

[21] Nielsen, M. A., "Cluster-state quantum computation," *Reports on Mathematical Physics*, Vol. 57, 2005, pp. 147–161. doi:10.1016/S0034-4877(06)80014-5.

[22] Kitagawa, M. and Ueda, M., "Squeezed spin states," *Phys. Rev.*, Vol. A47, 1993, pp. 5138–5143. doi:10.1103/PhysRevA.47.5138.

[23] Perelomov, A., *Generalized Coherent States and their Applications*, Springer-Verlag, New York, NY, 1972.

[24] Arrechi, F. T., Courtens, E., Gilmore, R., and Thomas, H., "Atomic coherent states in quantum optics," *Phys. Rev.*, Vol. A6, 1972, pp. 2211–2237. doi:10.1103/PhysRevA.6.2211.

[25] Radcliffe, J. M., "Some properties of coherent spin states," *J. Phys. A: Gen. Phys.*, Vol. 4, 1971, pp. 313. doi:10.1088/0305-4470/4/3/009.

[26] MacWilliams, F. J. and Sloane, N. J. A., *The Theory of Error-Correcting Codes*, North Holland, New York, NY, 1977.

[27] Horadam, K. J., *Hadamard Matrices and Their Applications*, Princeton University Press, Princeton, NJ, 2007.

[28] Deutsch, D. and Jozsa, R., "Rapid solution of problems by quantum computation," *Proc. Royal Soc. Lond. A*, Vol. 439, December 1992, pp. 553–558. doi:10.1098/rspa.1992.0167.

[29] Hall, M., "Semi-automorphisms of Hadamard Matrices," *Mathematical Proceedings of the Cambridge Philosophical Society*, Vol. 77, 1975, pp. 459–473. doi:10.1017/S0305004100051288.

[30] Michelson, A. M. and Levesque, A. H., *Error Control Techniques for Digital Communication*, John Wiley and Sons, New York, NY, 1985.

[31] Nielsen, M. A. and Chuang, I. L., *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge UK, 2000.

[32] Atallah, M. J., *Algorithms and Theory of Computation Handbook*, CRC Press LLC, Boca Raton, FLA, 1998.